EURO-ATLANTIC RESILIENCE TO DISINFORMATION IN THE DIGITAL AGE: A COMPARATIVE ANALYSIS OF EXISTING FRAMEWORKS

Daniela MUNTEANU
Euro-Atlantic Resilience Centre, Bucharest, Romania
daniela.munteanu@e-arc.ro
PhD candidate, National University of Political Studies and Public Administration, Bucharest, Romania
daniela.munteanu@comunicare.ro

Abstract: The evolving landscape of digital information presents a formidable challenge to democratic resilience, particularly within the transatlantic space. This paper analyses the dynamics of information governance in the wake of 2025's geopolitical strategic shifts and the rise of extremism across European Union (EU) member states. It critically examines the divergences in US and EU regulatory responses, the implications of corporate influence on digital governance, and the vulnerabilities stemming from AI-empowered information manipulation in democratic societies. By analysing and evaluating existing frameworks such as the EU's Digital Services Act, NATO's approach to disinformation, and their translation into national (non)regulatory measures, we reflect on tailored policy recommendations for strengthening democratic resilience in the digital age. The findings emphasise the necessity of enhanced transatlantic cooperation, reinforced platform accountability, and institutionalised digital security measures to counteract foreign and domestic threats to the integrity of public discourse.
Keywords: (dis)information, resilience, digital, governance, democratic, manipulation, cooperation, AI, transatlantic

INFORMATION ECOSYSTEMS AND DIGITAL GOVERNANCE

Information ecosystems have become a central battleground for the defence of democratic institutions, with state and non-state actors increasingly weaponising digital spaces to manipulate public perception. The 2024 electoral megacycle exposed the rapid evolution of disinformation tactics, particularly the rise of AI-generated content, platform-driven algorithmic manipulation, and foreign influence operations aimed at destabilising Western democracies. Against this backdrop, transatlantic efforts to mitigate "infothreats" remain hampered by fragmented digital governance approaches, as well as fundamental policy divergences in the Euro-Atlantic realm.

To explore the resilience frameworks addressing digital disinformation in the Euro-Atlantic space, this study applies a comparative and qualitative methodological approach. It synthesises strategic documents, academic literature, and case studies from selected states and institutions, including the EU, NATO, and national governments. This approach enables triangulation of empirical data and strategic insights to identify divergences in regulatory efforts and propose policy-relevant recommendations.

In terms of clarifying the concept, "digital governance" refers to the development and application by governments, the private sector and civil society, in their respective roles, of

shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the digital environment (Council of Europe, 2025).

Nowadays, information circulates from traditional to digital platforms instantly, sometimes bleeding untraceably and non-transparently into the information ecosystem. Although Internet users are not always aware, each of them is also a ”digital citizen” (Richardson & Milovidov, 2019) with a well-rounded virtual profile, put together through data collection of their activity online, which is then used to create targeted, tailored messages. These digital profiles are exploited by actors keen on determining behaviours and manipulating thoughts to their benefit and, oftentimes, to the detriment of the target. Communication is, therefore, weaponised, engineered as an offensive weapon.

To navigate the complexities of this battleground, a comprehensive regulatory approach should be taken into account, establishing a form of governance of the information ecosystems. The more encompassing governance of information ecosystems refers to the set of policies, institutional arrangements, and collaborative practices aimed at ensuring the resilience, integrity, and accountability of the networks in which information is generated, disseminated, and consumed. These ecosystems comprise both digital and traditional media channels, involving not only governmental actors but also private companies, civil society organisations, and transnational bodies (Mansell et al., 2025). In essence, governance of information ecosystems addresses the normative and operational frameworks designed to tackle challenges such as disinformation, foreign interference, and the broader destabilisation of public trust.

Against this backdrop, the 2024-2025 power transfer in the Euro-Atlantic world marked a pivotal shift in the geopolitical landscape, significantly impacting regulatory posture towards digital governance. The US rollback of platform accountability measures and the appeasement approach to Russia created new vulnerabilities in counter-disinformation efforts. Simultaneously, the rise of extremist and ultranationalist parties was backed by their presence on social platforms and the employment of bots, trolls, as well as AI-generated, fake content, building upon global conspiracies and Russian narratives that had been around for decades (European External Action Service, 2025b, 2024).

The presence and rampant growth of this phenomenon within all EU member states were met differently in terms of reaction speeds and receptivity to managing the phenomenon (Federal Ministry of the Interior and Community, 2025; Romanian Presidential Administration, 2024). Therefore, this constituted a factor which further fragmented Europe’s approach to digital regulation and security. These developments have exacerbated the already-prevalent challenges of coordinating international responses to disinformation, as malign actors exploit regulatory gaps to spread divisive narratives across both continents.

The rapid evolution of digital disinformation tactics has outpaced regulatory and institutional responses, placing democratic societies in a perpetual state of vulnerability. Over the past years, AI-generated disinformation promoting insidious political narratives has enabled malicious actors to manipulate voter sentiment with unprecedented precision (Chesney & Citron, 2019). The 2024 elections have demonstrated that AI-generated disinformation, deepfake technologies, and algorithmic content amplification have become central tools in digital influence campaigns.

These digital tools allowed for micro-targeting strategies that exploit voter psychology, ensuring that disinformation spreads more effectively through personalised messaging and social media algorithms (Wardle & Derakhshan, 2017). Political campaigns and state-sponsored actors have leveraged these advances to influence election outcomes, often bypassing traditional media verification mechanisms (European Commission, 2020a). These challenges have been exacerbated by the continued fragmentation of the information landscape, coupled with an increase in populist rhetoric that undermines the credibility of democratic institutions.

One of the most concerning developments in this regard has been the approach of some of the new decision-makers towards disinformation and extremist support. By normalising the spread of falsehoods under the pretence of free speech and cultivating an environment of distrust towards mainstream media and democratic institutions, sovereigntist influencers and administrations laid the groundwork for an information disorder that persists beyond their tenure. The weaponisation of digital platforms by political actors and foreign adversaries has further complicated efforts to ensure electoral integrity, leading us to a 2025 that brings about the shift of global power architecture and, at times, a visible lack of political will for truth and democracy, professed through telegraphic, manipulatory messaging on social media platforms.

Therefore, our study analyses existing transatlantic approaches to the governance of information ecosystems. We look at how freedom of speech and digital safety are interpreted on both sides of the Atlantic and how tensions rising from the different understanding of these concepts reflect on the realities of democracy. Our findings highlight the urgent need for greater transatlantic coordination, the enforcement of uniform regulatory standards, and the expansion of intelligence-sharing mechanisms to mitigate the impact of disinformation on democratic governance. The paper concludes by outlining a roadmap for future cooperative strategies, emphasising the role of diplomatic engagement, public-private partnerships, and the necessity of adapting legislative frameworks to counter the ever-evolving nature of digital threats.

EVOLVING DIGITAL DISINFORMATION TACTICS AND ELECTORAL MANIPULATION

The 2024 electoral cycle witnessed an unprecedented level of AI-driven content manipulation, where deepfake technology was used to generate false political narratives (Hubbard, 2024). The dissemination of these narratives was amplified through coordinated inauthentic behaviour on social media platforms, exploiting algorithmic biases to target specific voter demographics (Romanian Presidential Administration, 2024).

The rapid advancement of artificial intelligence (AI) and digital communication technologies has significantly transformed the nature of disinformation. The intersection of AI-generated deepfake content, social media manipulation, and hybrid warfare tactics has enabled state and non-state actors to launch sophisticated influence campaigns designed to destabilise democratic institutions and electoral processes. These efforts have intensified in 2024, as major elections across multiple countries provided fertile ground for coordinated disinformation attacks (European Union External Action, 2024).

Disinformation actors leveraged state-sponsored campaigns, primarily emanating from Russia and China, to manipulate public discourse in the United States and Europe. These influence operations were aimed at deepening political polarisation, eroding trust in democratic

processes, and suppressing voter participation (Ghosh & Scott, 2018). Concurrently, extremist groups within democratic societies exploited digital platforms to spread radicalising content under the guise of political advocacy.

Hybrid warfare strategies, combining cyber-attacks with targeted disinformation campaigns, have also been deployed to disrupt electoral processes in Romania, Ukraine, Georgia, and the Republic of Moldova (Martinescu et al., 2024; Pop, Dunai & Ivanova, 2024; Romanian Presidential Administration, 2024). Cyber intrusions targeting voter registration systems, political party networks, and electoral commission databases have been used in conjunction with disinformation efforts to sow doubt about election security (Kaska, Beckvard & Minárik, 2019; Martinescu et al., 2024; Romanian Presidential Administration, 2024). This hybrid approach was notably observed in the 2024 Ukrainian elections, where Russian-backed disinformation narratives falsely claimed election fraud and voter suppression in an attempt to delegitimise democratic institutions (European Union External Action, 2024).

Nevertheless, while AI technologies have enabled the proliferation of deepfakes and hyper-targeted disinformation, AI also presents critical opportunities for resilience. Automated detection systems using machine learning algorithms are now deployed to identify synthetic media and coordinated inauthentic behaviour at scale (Chatzakou et al., 2017). Moreover, natural language processing (NLP) models are being refined to trace disinformation narratives across platforms, offering proactive tools for moderation and policy enforcement (Jahn, Rendsvig & Stærk-Østergaard, 2023).

Over the past few years, we have seen a constant improvement of AI use for detecting and limiting inauthentic online behaviour, as well as regulatory advancements, including the implementation of the Digital Services Act (DSA) in the European Union. Nevertheless, enforcement disparities and platform resistance to stringent moderation policies have hindered progress. The limitations of self-regulatory measures in the United States, which rely on corporate goodwill rather than legal mandates, have also proven ineffective in addressing systemic disinformation threats (Gentile & Pollicino, 2025).

EURO-ATLANTIC FRAMEWORKS REGULATING THE DIGITAL INFOSPHERE

Actors ranging from the European Union to NATO emphasise robust "cyber diplomacy" and multi-stakeholder engagement as indispensable tools in confronting the proliferation of manipulative content (NATO, 2023a). Consequently, governance extends beyond static legislation: it requires adaptive strategies, agile institutions, and cross-sector collaborations – factors underscored by frameworks such as the EU's Action Plan Against Disinformation (European Commission, 2018b) and NATO's focus on hostile information activities (NATO, 2023a).

Effective governance of information ecosystems also encompasses strengthening societal resilience through media literacy and public awareness campaigns, especially in environments where harmful or misleading content circulates at scale (Wardle & Derakhshan, 2017). Measures such as heightened platform accountability, real-time fact-checking, and enhanced transparency in political advertising have been proposed to minimise the negative impact of disinformation (European Commission, 2020a). Overall, governance of information

ecosystems entails not only a regulatory mandate but also a commitment to preserving the democratic values and participatory rights that underpin pluralistic societies – particularly in periods of heightened electoral activity, where information flows directly shape political decision-making.

Unfortunately, the approach of some administrations coming into power over the past year was characterised by the deliberate use of falsehoods as a political strategy, undermining confidence in democratic institutions and instilling the ”post-truth” era. The repeated delegitimisation of electoral processes and media credibility fostered an environment where disinformation thrives. The persistence of narratives surrounding electoral fraud and deep-state conspiracies has continued to serve as a catalyst for extremist mobilisation, posing long-term threats to democratic stability.

Moreover, the recent US opposition to platform moderation policies emboldened extremist actors, normalising hate speech and coordinated online harassment. The absence of a federal regulatory framework to address disinformation has left the United States reliant on voluntary industry initiatives, which have proven insufficient in mitigating large-scale influence operations.

While the EU has implemented comprehensive regulatory frameworks, Single Market For Digital Services (European Commission, 2020b), the iterations of the Code of Practice on Disinformation (European Commission, 2018a; European Comission, 2022), the DSA, the spread of disinformation remains a critical challenge. Foreign information manipulation and interference (FIMI) (European Union External Action, 2023), particularly from Russia and China (European External Action Service, 2025a; European Union External Action, 2024, 2023), has sought to exploit existing societal divisions within democratic states (European Parliament, 2023b; European Union External Action, 2024). In contrast to the United States’ decentralised approach to content regulation, the EU’s enforcement of digital governance measures has demonstrated greater consistency, although the implementation of these policies varies among member states.

THE EUROPEAN UNION’S APPROACH TO THE DIGITAL INFOSPHERE

Aiming to limit the nefarious effects of information manipulation that Europe had been a victim of – especially since the invasion of Crimea – and that had exploded during the COVID-19 pandemic, policymakers and stakeholders sought to balance regulatory measures with the foundational values of democracy. The process was not straightforward, especially in the case of the European Union, which is a complexly articulated organisation and greatly values the right to freedom of expression.

Since the early 2010s, the European Union has progressively developed and refined its approach to managing the information ecosystem inhabited by its citizens. The first major step in this direction was the establishment of the European External Action Service’s (EEAS) East StratCom Task Force in 2015, aimed at countering Russian disinformation campaigns. This initiative was followed by the 2018 Action Plan Against Disinformation, which sought to increase cooperation among member states in tackling false narratives and bolstering societal

resilience (European Commission, 2018b). The EU's Action Plan against Disinformation is central to the broader effort to regulate and combat information manipulation because it provides a cohesive, EU-wide framework for identifying, preventing, and responding to the spread of false or misleading content (see Table 1 below). It is the first key initiative jumpstarting EU's ensuing broader set of efforts aimed at safeguarding democratic and societal resilience to disinformation.

Table 1. The EU's approach to disinformation

The EU's *Action Plan against Disinformation*		
Key provisions	**Argument**	**Implementation**
Coordinated Response Across Member States	Disinformation often crosses national boundaries and exploits fragmented regulatory environments.	By harmonising approaches, the Action Plan helps member states share data, best practices, and early warnings, ensuring a unified response to ongoing and emerging threats.
Protecting Democratic Processes	Disinformation can undermine free and fair elections, polarise debate, and erode trust in democratic institutions.	The Action Plan sets out targeted measures to safeguard electoral processes, including greater transparency around political advertising and campaign financing on digital platforms.
Clear Accountability for Online Platforms	The Action Plan strengthens the EU's role in holding major tech and social media companies accountable for illegal or harmful content.	It ties into and complements subsequent initiatives (like the Digital Services Act and the revised Code of Practice on Disinformation) that require platforms to remove or reduce the spread of misleading or harmful information.
Building Societal Resilience	Beyond immediate enforcement efforts, the plan emphasises media literacy, critical thinking, and awareness-raising across European societies.	It supports independent fact-checkers, researchers, and civil society organisations, thus fostering a more informed public better able to recognise and resist manipulative content.
Early Detection and Rapid Response	A key element of the plan is creating better tools and networks for identifying disinformation campaigns early.	Through initiatives like the Rapid Alert System, the EU strengthens cross-border coordination so that threats can be addressed before they do extensive harm.

Taken together, these elements (see Table 1) make the Action Plan against Disinformation an essential pillar of the EU's broader regulatory strategy to tackle information manipulation. By setting out clear guidelines, coordination mechanisms, and accountability requirements, the plan helps safeguard Europe's democratic processes and promotes a more transparent, trustworthy online environment.

In 2020, the European Democracy Action Plan (EDAP) expanded these efforts, introducing measures to protect election integrity, improve media freedom, and enhance digital literacy (European Commission, 2020a). Alongside this, the Code of Practice on Disinformation was adopted as a self-regulatory framework for online platforms in 2018 and enhanced in 2022, encouraging greater transparency and proactive measures to limit the spread of false information (European Commission, 2018a; European Comission, 2022).

The Digital Services Act (DSA), which came into effect in 2024, represented the most ambitious attempt yet to regulate the online information space (see Table 2). The legislation mandated increased platform accountability, requiring major digital services to implement risk assessment mechanisms and enforce stricter moderation policies against disinformation (Anon, 2022a). However, enforcement remained a challenge, with disparities in national implementation slowing its effectiveness.

Table 2. EU regulation of the infospace

The Eu's *Digital Services Act*	
Key provisions	**Implementation**
Transparency requirements on platform mechanisms, advertiser and publisher transparency	- mandates greater transparency from online platforms regarding their content moderation practices, algorithms for content recommendation, and advertising systems; - requires platforms to disclose why users are seeing certain ads and who is paying for those ads; - requires platforms to explain how these systems work in a way that is understandable to the average user;
Protection against illegal content	sets out clear obligations for the removal of illegal content while safeguarding users' rights, including the establishment of an effective mechanism for users to report such content and for platforms to cooperate with national authorities
Empowerment of users	users are given more control over what they see online, including options to opt-out of algorithmic recommendations and easier ways to report harmful content
Accountability measures	online platforms, especially very large ones, are required to undergo independent audits to assess compliance with the DSA's obligations- this includes assessing risks to societal harms and the effectiveness of their systems to mitigate these risks

The rise of artificial intelligence (AI)-generated disinformation and the increasing involvement of foreign actors in election manipulation necessitated further action. In response, the European Union published its Reports on Foreign Information Manipulation and Interference (FIMI) (European Parliament, 2023b, 2023a), identifying key vulnerabilities in its regulatory framework and recommending closer coordination with NATO and transatlantic partners (European Union External Action, 2024, 2023).

Despite these efforts, foreign information manipulation and interference, particularly from Russia and China, has continued to exploit societal divisions within democratic states. The divergence in regulatory approaches between the EU and the United States following the 2025 Trump administration's rollback of content moderation policies (Datta, 2025; Malingre, 2025; Ray, 2025; Windwehr, 2025; Gentile & Pollicino, 2025; Richter et al., 2025) further weakened joint efforts to combat digital disinformation and strained US-EU relations on digital space cooperation. The lack of a unified approach created loopholes that adversarial states readily exploited, undermining trust in democratic institutions and fuelling polarisation.

In the face of these challenges, EU member states should intensify national interventions and strategic efforts, while establishing EU hybrid threat response units, strategic communication departments, integrated and clear coordination mechanisms, as well as funding for media literacy programs. Nevertheless, without stronger enforcement mechanisms and deeper transatlantic cooperation, the resilience of the European information ecosystem remains in question.

NATO's Strategic Response to Disinformation

For over a decade, NATO has progressively recognised disinformation as a core component of hybrid warfare, leading to the development of a series of initiatives aimed at strengthening

resilience among member states. One of the earliest strategic responses was the establishment of the NATO Strategic Communications Centre of Excellence (StratCom COE) in 2014, tasked with analysing and exposing hostile information activities. This initiative was followed by the adoption of enhanced cooperation mechanisms with the European Union, in order to improve information sharing and help build broader awareness of the threat landscape (Johns Hopkins University, Imperial College London & Georgia Institute of Technology, 2021; NATO, 2023a, 2023c).

The NATO 2030 Initiative, launched in 2020, further reinforced the alliance's focus on disinformation as a strategic threat. The initiative emphasised the need for comprehensive resilience-building measures, including increased investments in cybersecurity, strategic communication, and coordinated responses to foreign information manipulation (Reflection Group Appointed by the Secretary General, 2020). This was complemented by NATO's 2021 Brussels Summit Declaration, which reaffirmed the alliance's commitment to protecting democratic institutions from malign information activities (NATO, 2021).

NATO has increasingly recognised that disinformation is a multidimensional threat capable of undermining democratic principles, eroding trust in public institutions, and weakening collective defence (NATO, 2023a). While NATO does not enact legislation akin to national or EU regulations, it has initiated a series of strategic frameworks and capacity-building measures aimed at enhancing Allied resilience to hostile information operations. A critical example is NATO's comprehensive "hostile information activities" doctrine, whereby disinformation is treated as part of a wider set of hybrid threats designed to exploit social and political fissures among member states (NATO, 2025). This doctrinal approach underscores the Alliance's acknowledgement that disinformation can function as an asymmetric weapon, operating in conjunction with cyber-attacks, economic coercion, and other destabilising tactics (NATO, 2024a).

A foundational element in this effort is the establishment of specialised Centres of Excellence (CoEs), such as the NATO Strategic Communications Centre of Excellence (StratCom CoE) in Riga and the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. These institutions serve as hubs for research, training, and policy development, focusing on understanding, detecting, and countering adversarial narratives. They provide analytical tools, conduct regular "red team" exercises, and offer strategic guidance to NATO member states (Reflection Group Appointed by the Secretary General, 2020). By facilitating cross-national collaboration, they allow for the rapid exchange of information and best practices, enabling Allies to respond to disinformation campaigns more effectively.

Another key initiative lies in NATO's large-scale training exercises, including those that integrate scenarios involving disinformation as part of "hybrid warfare" (NATO, 2023b). These exercises test Allied capabilities in identifying and managing information manipulation in real time (NATO, 2023a). Through simulations involving bot-generated content, deepfake videos, or fabricated narratives about NATO missions, member states gain hands-on experience in recognising disinformation patterns and coordinating rapid responses. The impact of these exercises aims to extend beyond military circles by strengthening civilian and governmental preparedness, thereby fostering a more resilient public sphere.

Furthermore, strategic communications policies and public diplomacy efforts form part of NATO's broader goal to combat disinformation. NATO headquarters in Brussels and public

affairs offices across member states coordinate outreach strategies to address specific hostile narratives, ensuring that transparent, factual information is disseminated consistently (NATO, 2024b). The impact is twofold: first, it helps guard public confidence in collective defence mechanisms; second, it demonstrates to adversarial actors that NATO is prepared to counter influence campaigns swiftly and cohesively.

Overall, NATO's initiatives to increase resilience to disinformation combine doctrinal clarity, capacity-building institutions, and practical simulations of hybrid threats. Their intended impact is to preserve the credibility and unity of the Alliance, deter actors who seek to destabilise NATO through propaganda, and uphold democratic values by enhancing the public's ability to discern and resist manipulative content.

The U.S approach to disinformation: between self-regulation and legislative oversight

Unlike the EU's regulatory approach, the United States has relied heavily on platform self-regulation. Companies such as Meta, Twitter (now X), and Google have implemented content moderation policies, but their discretionary enforcement has led to accusations of bias and selective censorship (Cobbe, 2021; Gillespie, 2018; Krishnan et al., 2021). Additionally, the repeal of the Federal Communications Commission's net neutrality regulations in 2017 further enabled the spread of manipulative content by reducing oversight of digital information flows (Kang, 2017). Legislative measures such as the bipartisan Platform Accountability and Consumer Transparency Act/PACT Act (Coons, 2022) have attempted to impose greater responsibility on social media companies, but enforcement remains inconsistent. The failure to establish bipartisan consensus on the need for stricter regulations has allowed digital platforms to continue operating with limited accountability (Napoli, 2019). The lack of uniform federal guidelines has also contributed to an environment where states have taken divergent approaches to content moderation, leading to legal fragmentation and enforcement disparities (Richter et al., 2025). As yet another confirmation of the issue at hand, the recent Protect Elections Act (Cole, 2025), which has sought to establish clearer accountability measures, was met with partisan gridlock that impeded substantial regulatory progress.

COMPARATIVE ANALYSES OF REGULATORY FRAMEWORKS' IMPLEMENTATION IN EURO-ATLANTIC DIGITAL INFORMATION ECOSYSTEMS

The European approach: progress at different speeds

In the run-up to the European Parliament elections, coordinated disinformation efforts sought to amplify anti-EU sentiments through targeted social media campaigns. These narratives, often linked to Russian and Chinese state-sponsored media, promoted conspiracy theories about EU governance, attempting to reduce voter turnout and discredit democratic institutions (European Union External Action, 2024). The European Commission responded by raising awareness through EEAS's flagship project EuvsDisinfo (Anon, 2025a), as well as by launching several public communication campaigns and collaborating with tech platforms to de-platform known sources of manipulated content (European Commission, 2025).

France's presidential election, as well as last year's EU and legislative ballot, also faced major disinformation threats, particularly from far-right extremist groups leveraging AI-powered propaganda to spread xenophobic and anti-immigration narratives (Quinn & Milmo,

2024). Using its 2018 Anti-Disinformation Law (Jeangène Vilmer et al., 2018), the French government coordinated with fact-checking organisations and social media platforms to contain the spread of false information, demonstrating the effectiveness of a well-regulated digital information space.

Romanian presidential elections in November 2024, on the other hand, presented the country and international community with a shock: a candidate that had been barely known up to a month before the ballot, with popularity percentages in the one-digit range, came in first in the first electoral round. According to research powered by AI threat detectors, the obscure candidate's sudden surge in popularity was the result of a carefully orchestrated social media strategy. Independent researchers identified 614 networks (webpages, websites, social media channels, accounts) that amplified Călin Georgescu's profile and narratives across a vast ecosystem of social media platforms (i.e.: Telegram, Facebook, Twitter/X i.e.). These networks – predominantly Russian-affiliated – span multiple continents and languages (Martinescu et al., 2024:p.2).

Romanian governmental authorities, who had recently implemented the DSA provisions, noticed the nefarious activity and contacted TikTok to require appropriate labelling of political content and compliance with EU and the platform's own regulations (Digi24, 2024). Nevertheless, TikTok refused to acknowledge the fact that it hosts political content and, therefore, did not offer any transparency on the information manipulation at work behind the coordinated campaign artificially increasing Călin Georgescu's popularity and profile. Among rising hybrid threats and aggressive information manipulation against democracy and the Romanian society, X owner, Elon Musk, repeatedly attacked Romanian courts' decisions and ANCOM, the Romanian authority on digital services that has been fighting to safeguard the Romanian infospace from nefarious manipulative activity (Digi24, 2025, Anon, 2025b).

A more successful example of a national approach to safeguard democratic resilience and stave off FIMI was provided by the German Bundestag elections in February 2025. Aside from discursive manipulation, the Alternative für Deutschland (AfD) – a far-right extremist party with an anti-immigrant stance – has been an avid user of AI image generators. In September, the AfD's Brandenburg branch produced AI-made campaign adverts that contrast an idealised Germany featuring blond-haired and blue-eyed people with scenes of veiled women walking down streets and a person waving an LGBTQ+ flag. Other pro-AfD groups on Facebook used AI images emblazoned with nativist or anti-immigrant slogans, while another showed a giant pig – an animal whose meat is prohibited from consumption in Islam – chasing a group of people in Islamic clothing, with the slogan "Arabic film version of Godzilla". With a good public communication campaign, designed to raise awareness on the treacherous nature of extremist propaganda and information manipulation, the German voters mobilised in an exemplary manner, so that any possible attempt of foreign interference (European External Action Service, 2025b) would be greatly reduced. Aside from effective, timely and convincing communication on the part of authorities and civil society entities promoting democracy, the state had previously set a broader framework to manage threats to the information ecosystem. One notable effort in this direction was the establishment of the Central Office for the Detection of Foreign Information Manipulation (ZEAM) – the Federal Government unit for the early detection of foreign influence and manipulation campaigns. ZEAM is the product of a joint initiative of the Federal Ministry of the Interior

and Community, the Federal Foreign Office, the Federal Ministry of Justice, and the Press and Information Office of the Federal Government. ZEAM's objective is to protect Germany's free and democratic constitutional system and its processes of political decision-making, such as elections, against manipulative and hidden influence by foreign countries (Federal Ministry of the Interior and Community, 2025).

The effectiveness of regulatory frameworks in mitigating the spread of disinformation has varied significantly across different governance models. The European Union's DSA has introduced comprehensive measures to enhance transparency and accountability for online platforms, but enforcement disparities among member states have created challenges in implementation (Munteanu, 2024). In contrast, the United States has taken a decentralised approach, relying on platform self-regulation, which has led to inconsistencies in content moderation practices (Krishnan et al., 2021). Some countries, such as Germany and France, have successfully integrated fact-checking partnerships and legal frameworks to combat disinformation, whereas others, like Romania and Hungary, have struggled either with creating an effective approach to countering FIMI or have even had government-aligned media amplifying misleading narratives (Anon, 2022b; Wonka, Gastinger & Blauberger, 2025).

Fact-checking organisations, media coalitions, and public awareness campaigns have played a critical role in countering disinformation and rebuilding trust in democratic institutions. Initiatives such as the European Digital Media Observatory (EDMO) and the International Fact-Checking Network (IFCN) have expanded their efforts to verify election-related claims and curb the spread of false information. Media literacy programs in schools and public institutions have also proven effective in equipping citizens with the skills needed to critically assess online content (Dobrescu, Durach & Vladu, 2022). However, the impact of these initiatives has been limited in countries with high media polarisation and limited press freedom (Castro et al., 2022; Garcia, 2024; Reporters Without Borders, 2020).

A comparative analysis of disinformation resilience across different governance models reveals important lessons for policymakers. Countries with strong institutional safeguards, such as France, Estonia and Germany, have demonstrated greater resilience due to proactive regulatory frameworks and well-integrated cyber defence mechanisms (Federal Ministry of the Interior and Community, 2025; Jeangène Vilmer et al., 2018; Kaska, Beckvard & Minárik, 2019). Conversely, countries with weaker institutional protections, such as Hungary and Romania, have faced heightened challenges in combating disinformation due to a lack of regulatory enforcement and pervasive foreign influence operations (European External Action Service, 2024; Pop, Dunai & Ivanova, 2024; Romanian Presidential Administration, 2024; Al Jazeera, 2024; Wonka, Gastinger & Blauberger, 2025). These variations highlight the need for adaptable policy strategies that account for the unique vulnerabilities of different political systems.

US democracy between platform overlords and regulatory roll-backs

The impact of disinformation campaigns has been evident in multiple high-profile elections, most recently creating tensions in the margins of the 2024-2025 ballots. The US presidential election, for example, saw an unprecedented wave of AI-generated disinformation, including fabricated news stories and manipulated videos falsely depicting candidates in compromising situations (U.S. Government Accountability Office, 2024). While US authorities implemented

countermeasures, including real-time fact-checking partnerships and cybersecurity enhancements, the volume and sophistication of digital manipulation posed significant challenges (Kovalčíková & Spatafora, 2024).

The significant challenges that the United States faced in regulating disinformation were doubled by political polarisation that exacerbated the debate over freedom of speech and platform governance. Some administrations' tenures were marked by systematic attacks on media credibility, the promotion of conspiracy theories, and the deliberate undermining of electoral integrity. This period saw the proliferation of misleading narratives amplified through social media platforms, facilitated by the rollback of regulatory oversight and the weakening of journalistic norms. The persistence of these narratives in the 2024 election cycle underscores the long-term consequences of disinformation-fuelled populism, particularly as then former President Trump and his team continued to challenge the legitimacy of the electoral process he had lost, while presently invoking the argument of freedom of speech to stifle platform regulation and reduce transparency of digital information (Richter et al., 2025).

The inauguration of Donald Trump for a second term in 2025 has further complicated the regulatory landscape for disinformation governance. The administration has moved to dismantle existing counter-disinformation initiatives, framing them as infringements on free speech. Efforts to curtail platform accountability measures, including provisions of the DSA, that the EU has sought to implement in transatlantic cooperation, have weakened US commitments to combating foreign information manipulation. Trump's reimplementation of executive orders targeting content moderation policies has emboldened platforms to relax their efforts in flagging or de-platforming sources known for spreading false narratives (Malingre, 2025).

The implications of these policy shifts extend beyond US borders, impacting the European information ecosystem. With the rollback of federal oversight on digital platforms, malign actors, particularly from Russia and China, have exploited regulatory gaps to influence transatlantic political discourse. FIMI campaigns targeting EU institutions, elections, and democratic processes have increased, facilitated by the lack of coordinated enforcement mechanisms between the US and its European allies (Datta, 2025; Gentile & Pollicino, 2025; Richter et al., 2025; Windwehr, 2025). The withdrawal of US engagement in joint fact-checking and intelligence-sharing initiatives has further strained global efforts to curb digital disinformation.

In this altered information landscape, European governments have intensified independent regulatory strategies to mitigate the risks of digital manipulation. However, the divergence in US and EU approaches to digital governance has introduced new challenges in international cooperation. Without US alignment on content moderation and disinformation policies, the efficacy of EU-led initiatives such as the DSA and NATO's counter-disinformation strategies is significantly diminished. The continued entrenchment of false narratives within the US public sphere, amplified by political leadership, poses a persistent risk to democratic resilience both domestically and abroad.

CHALLENGES IN BOLSTERING RESILIENCE TO DISINFORMATION

Despite advancements in regulatory frameworks, several transnational challenges remain that hinder a coordinated response to disinformation in both the US and the EU. Striking a balance between combating disinformation and safeguarding freedom of speech remains a contentious issue in both the United States and European Union, particularly as interpretations

of free expression differ significantly. Moreover, while the EU has implemented robust legal frameworks such as the DSA, enforcement varies across member states. In contrast, the US continues to rely on self-regulation, creating inconsistencies that foreign adversaries exploit. State-sponsored disinformation and hybrid warfare remain significant threats to democracies, as Russia and China continue to leverage digital platforms to manipulate political discourse in both the US and EU, highlighting the need for greater transatlantic intelligence-sharing and defensive mechanisms (European External Action Service, 2025). Above all these, trust in media and government institutions has plummeted over recent years (Fischer, 2024; Gallup, 2024). The proliferation of disinformation has significantly eroded public trust in democratic institutions on both sides of the Atlantic, undermining coordinated policy responses and crisis management efforts (Anon, 2018). Little progress can be achieved while large technology companies wield such influence in shaping digital governance policies, leading to lobbying efforts that often impede stringent regulatory measures.

The relationship between the United States and Russia has undergone significant shifts under the 2025 administration, further complicating efforts to build transatlantic resilience to disinformation. The administration's policy of rapprochement with Moscow, characterised by the rollback of sanctions and a reduction in counterintelligence efforts, has emboldened Russian information warfare strategies even since the first Trump administration (Klimburg, 2017). With less oversight on foreign digital interference, Russian state-sponsored disinformation has proliferated on US-based platforms, amplifying narratives that undermine European security policies and democratic cohesion within NATO.

This shift in US foreign policy has also weakened the EU's ability to counteract Russian disinformation campaigns. The absence of a unified transatlantic stance has led to increased divergence in European responses, as some member states advocate for stronger countermeasures while others hesitate due to economic dependencies on Russian energy or political alignment with pro-Kremlin factions (European Commission, 2024). The erosion of US-EU intelligence-sharing agreements has further impaired coordinated responses, allowing Russian influence operations to exploit existing vulnerabilities in the European digital space.

Compounding these challenges is the outsized role of corporate moguls in shaping the information environment. As the owner of critical communication infrastructures – including Starlink and social media platform X – Musk's influence extends beyond the technological sphere into geopolitical decision-making (Zuboff, 2023). His close ties with the Trump administration and outspoken support for populist and extremist candidates in EU member states, such as Romania's Călin Georgescu, have fuelled concerns over the private sector's role in exacerbating democratic instability (Krekó, 2025). Musk's control over digital communication networks has raised alarms within European security circles, as his platforms have been used to amplify nationalist rhetoric and anti-EU sentiments. His resistance to regulatory oversight has further strained relations with European policymakers, who view his laissez-faire approach to content moderation as a direct threat to information integrity. The proliferation of far-right narratives on his platforms has bolstered political movements that challenge EU cohesion, complicating efforts to implement coordinated disinformation countermeasures (Haggart, Scholte & Tusikov, 2024).

Given these shared vulnerabilities, a transatlantic strategy for countering disinformation must focus on greater regulatory harmonisation, enhanced cybersecurity cooperation, and

the establishment of joint task forces for real-time information-sharing. However, political challenges persist. The US's policy reversals have weakened the prospect of immediate cooperation, while differing national priorities among EU member states complicate the formulation of a unified response. Additionally, recent Russian escalating aggression towards European states hinders any chance of diplomatic efforts to address foreign influence operations.

Moving forward, successful transatlantic cooperation will depend on sustained diplomatic engagement, strengthened multilateral institutions, and the political will to prioritise digital resilience as a cornerstone of democratic security.

POLICY RECOMMENDATIONS FOR STRENGTHENING RESILIENCE TO DISINFORMATION

Given the complex challenges the information ecosystem is faced with, a robust policy approach must address both the structural weaknesses in transatlantic cooperation and the rapidly evolving digital landscape. The following recommendations could contribute to a structured transatlantic path toward strengthening resilience to disinformation.

While these recommendations provide a structured policy pathway, their implementation is contingent on the political landscape in both the US and the EU. The USA's strategic repositioning, characterised by a more isolationist stance and reduced regulatory intervention, may hinder immediate transatlantic cooperation. Meanwhile, the rise of extremist political figures in EU member states poses further challenges to achieving consensus on information governance policies. However, given the escalating threats posed by foreign influence operations and internal polarisation, the urgency of coordinated action cannot be overstated. Moving forward, democratic resilience will depend on the ability of policymakers to align strategies, leverage diplomatic channels, and prioritise the integrity of the digital information landscape.

CONCLUSIONS

The comparative analysis of Euro-Atlantic frameworks for managing disinformation reveals significant gaps and divergences that hinder the effectiveness of a coordinated response. While the European Union has adopted a robust regulatory approach through the DSA, the United States remains fragmented in its strategy, relying heavily on self-regulation and voluntary industry compliance. This lack of uniformity has created an uneven playing field where disinformation thrives, particularly as malign foreign actors exploit these regulatory discrepancies to disseminate false narratives.

The American administration's rollback of platform accountability measures and its renewed alignment with Russia have significantly weakened transatlantic cooperation on counter-disinformation efforts. By deprioritising regulatory oversight and intelligence-sharing agreements, the US has created additional vulnerabilities that adversarial states such as China and Russia continue to exploit, further destabilising the digital information space.

In contrast, the European Union's commitment to legislative action – exemplified by the enforcement of the DSA – has positioned it as a global leader in combating disinformation. However, internal political fragmentation caused by the rise of extremist political movements in several EU member states has weakened collective enforcement mechanisms. Figures such as Romania's Călin Georgescu and other far-right actors have leveraged digital platforms to spread nationalistic rhetoric, demonstrating the persistent challenge of curbing homegrown FIMI campaigns alongside external threats.

The role of corporate actors, particularly figures like Elon Musk, has further complicated the landscape. Musk's control over critical digital infrastructure, such as Starlink and social media platform X, has demonstrated how privatised power can influence geopolitical narratives. His alignment with Trump's deregulatory stance and his overt support for extremist candidates in Europe have amplified disinformation risks, reinforcing the necessity of stronger regulatory oversight on technology moguls with outsized influence in the information space.

Another crucial takeaway from this research is the growing importance of NATO's role in counter-disinformation strategies. While NATO has historically focused on military threats, the increasing weaponisation of digital platforms has necessitated a broader approach to hybrid warfare. The integration of disinformation resilience into NATO's strategic framework remains critical, yet its effectiveness is contingent on the willingness of member states to align their policies and intelligence-sharing mechanisms.

Moving forward, policy recommendations (see Table 3) emphasise the need for greater harmonisation between US and EU regulatory frameworks. A transatlantic disinformation task force, enhanced diplomatic engagement, and cross-sector cooperation with independent fact-checkers and civil society organisations are vital components of a successful resilience strategy. Additionally, the expansion of counter-disinformation diplomacy to include stronger international sanctions against state-sponsored campaigns would provide a more comprehensive deterrent against foreign influence operations.

Table 3. Policy Recommendations for Strengthening Resilience to Disinformation

Resilience building measure	Rationale
Enhance Platform Accountability through Regulatory Convergence	The US should consider adopting elements of the EU's Digital Services Act (DSA), enforcing transparency requirements for social media algorithms and content moderation decisions. Such a move would reduce discrepancies between regulatory frameworks and ensure a more unified approach to tackling harmful digital content.
Expand Counter-Disinformation Diplomacy	Transatlantic diplomatic engagement should prioritise countering the influence of adversarial states such as Russia and China. A formal commitment within NATO to treat disinformation as a core security threat would further solidify the integration of resilience into broader defence strategies
Introduce Sanctions for State-Sponsored Disinformation Campaigns	Both the US and the EU should impose targeted economic sanctions on entities and individuals responsible for orchestrating disinformation campaigns. A framework akin to the EU's FIMI Reports should be established in the US to ensure accountability
Regulate Tech Mogul Influence on Digital Governance	Policies should be enacted to limit the unchecked influence of technology magnates on digital information ecosystems. Digital overlords' control over communication platforms has highlighted the risks of privatised geopolitical influence, necessitating stronger oversight mechanisms to ensure fair governance
Strengthen Electoral Integrity Measures	Given the role of disinformation in undermining electoral processes, both the US and the EU should enhance election security protocols. These measures should include AI-driven monitoring of online election-related discourse and rapid-response teams to address emerging disinformation threats.
Encourage Cross-Sector Cooperation Between Governments and Civil Society	Collaboration between policymakers, academia, and civil society groups is crucial in fostering an agile response to evolving disinformation tactics. EU-led initiatives such as the European Digital Media Observatory could be expanded to include US participation

A major challenge remains the political feasibility of these measures in the current geopolitical context. While the EU continues to push for stricter platform accountability, the US political climate – characterised by ideological polarisation and corporate lobbying – complicates the prospects for similar regulatory progress. The return of Trump has further entrenched divisions, making it unlikely that a bipartisan consensus on digital governance will be achieved in the near future.

Nonetheless, the urgency of addressing these vulnerabilities cannot be overstated. With AI-generated disinformation accelerating at an unprecedented rate, democratic institutions must prioritise proactive strategies over reactive measures and dive deeper into the opportunities represented by AI LLM analysis, moderation and regulation of online content. Public-private partnerships, targeted legislative reforms, and sustained intelligence-sharing are essential to countering the rapidly evolving digital threats to democratic integrity.

Ultimately, the transatlantic alliance must recognise that disinformation is not merely a political issue but a fundamental security threat. Strengthening resilience requires not only legislative action but also cultural and institutional shifts that promote critical thinking, digital literacy, independent media sustainability, and robust fact-checking mechanisms. Without decisive action, the erosion of public trust in democratic processes will continue, leaving societies increasingly vulnerable to the destabilising forces of digital manipulation.

REFERENCE LIST

Al Jazeera (2024) Romania's top court annuls results of presidential election's first round. *Al Jazeera*. 6 December. https://www.aljazeera.com/news/2024/12/6/romanias-top-court-annuls-results-of-presidential-elections-first-round.

Anon (2022a) *Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. (*2022/2065*). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.

Anon (2025a) *EUvsDisinfo | Detecting, analysing, and raising awareness about disinformation*. 2025. EUvsDisinfo. https://euvsdisinfo.eu/ [Accessed: 25 March 2025].

Anon (2025b) *Romanian media watchdog defies Musk over censorship claims*. 24 March 2025. POLITICO. https://www.politico.eu/article/romanian-social-media-watchdog-defies-elon-musk-censorship-speech-claims/ [Accessed: 25 March 2025].

Anon (2022b) *The DSA Proposal and Hungary - DSA Observatory*. 11 March 2022. https://dsa-observatory.eu/2022/03/11/the-dsa-proposal-and-hungary/.

Y. Benkler, R. Faris, & H. Roberts (eds.) (2018) Copyright Page. In: *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press. p. 0. doi:10.1093/oso/9780190923624.002.0003.

Castro, L., Strömbäck, J., Esser, F., Van Aelst, P., De Vreese, C., Aalberg, T., Cardenal, A.S., Corbu, N., Hopmann, D.N., Koc-Michalska, K., Matthes, J., Schemer, C., Sheafer, T., Splendore, S., Stanyer, J., Stępińska, A., Štětka, V. & Theocharis, Y. (2022) Navigating High-Choice European Political Information Environments: a Comparative Analysis of News User Profiles and Political Knowledge. *The International Journal of Press/Politics*. 27 (4), 827–859. doi:10.1177/19401612211012572.

Chatzakou, D., Kourtellis, N., Blackburn, J., De Cristofaro, E., Stringhini, G. & Vakali, A. (2017) Mean Birds: Detecting Aggression and Bullying on Twitter. In: *Proceedings of the 2017 ACM on Web Science Conference*. WebSci '17. 25 June 2017 New York, NY, USA, Association for Computing Machinery. pp. 13–22. doi:10.1145/3091478.3091487.

Chesney, B. & Citron, D. (2019) Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*. 107, 1753.

Cobbe, J. (2021) Algorithmic Censorship by Social Platforms: Power and Resistance. *Philosophy & Technology*. 34 (4), 739–766. doi:10.1007/s13347-020-00429-0.

Cole, T. (2025) *Protect American Election Administration Ac*t. http://cole.house.gov/media/press-releases/cole-introduces-protect-american-election-administration-act-2025.

Coons, C.A. (2022) *Platform Accountability and Transparency Act*. https://www.congress.gov/bill/117th-congress/senate-bill/5339/text.

Council of Europe (2025) *Digital Governance*. 2025. Digital Governance. https://www.coe.int/en/web/digital-governance/overview [Accessed: 15 March 2025].

Datta, A. (2025) *Trump threatens to launch tariff attack on EU tech regulation*. 22 February 2025. Euractiv. https://www.euractiv.com/section/tech/news/trump-threatens-to-launch-tariff-attack-on-eu-tech-regulation/ [Accessed: 16 March 2025].

Digi24 (2025) *ANCOM răspunde acuzațiilor lui Musk privind cenzura și dezvăluie detalii despre testele Starlink în România: „Ne datorează mai mult”*. https://www.digi24.ro/stiri/externe/ancom-raspunde-acuzatiilor-lui-musk-privind-cenzura-si-dezvaluie-detalii-despre-testele-starlink-in-romania-ne-datoreaza-mai-mult-3170063.

Digi24 (2024) *ANCOM: TikTok nu a acţionat la solicitarea AEP ce semnala diverse nereguli legate de conţinutul ilegal distribuit*. https://www.digi24.ro/alegeri-prezidentiale-2024/ancom-tiktok-nu-a-actionat-la-solicitarea-aep-ce-semnala-diverse-nereguli-legate-de-continutul-ilegal-distribuit-3022139.

Dobrescu, P., Durach, F. & Vladu, L. (2022) *Building Resilience to Disinformation Through Media and Information Literacy*. In: 1 March 2022 pp. 3059–3068. doi:10.21125/inted.2022.0863.

European Comission (2022) *2022 Strengthened Code of Practice on Disinformation | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

European Commission (2018a) *2018 Code of Practice on Disinformation | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

European Commission (2018b) *Action Plan against Disinformation*. doi:10.1093/law-oeeul/e66.013.66.

European Commission (2020a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.

European Commission (2025) *Countering information manipulation*. February 2025. https://commission.europa.eu/topics/countering-information-manipulation_en [Accessed: 17 March 2025].

European Commission (2020b) Single Market For Digital Services (Single Market Act) and amending Directive 2000/31/EC. *2020/0361* (*COD*). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.

European External Action Service (2025a) *3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

European External Action Service (2024) *Disinfo: The EU interfered in the Romanian elections*. https://euvsdisinfo.eu/report/the-eu-interfered-in-the-romanian-elections/.

European External Action Service (2025b) P*ro-Kremlin outlets drool over German elections*. 20 February 2025. EUvsDisinfo. https://euvsdisinfo.eu/pro-kremlin-outlets-drool-over-german-elections/ [Accessed: 15 March 2025].

European Parliament (2023a) *Foreign interference in EU democratic processes: Second report*.

European Parliament (2023b) *Report on foreign interference in all democratic processes in the European Union, including disinformation*. (A9-0187/2023). https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.pdf.

European Union External Action (2023) *1st EEAS Report on Foreign Information Manipulation and Interference Threats*. p. 36. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

European Union External Action (2024) *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.

Federal Ministry of the Interior and Community (2025) *Protecting the 2025 Bundestag elections from hybrid threats and disinformation*. https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html?nn=9386226.

Fischer, S. (2024) *Media trust hits another historic low*. 15 October 2024. Axios. https://www.axios.com/2024/10/15/media-trust-gallup-survey [Accessed: 25 March 2025].

Gallup (2024) *Americans' Trust in Media Remains at Trend Low*. 14 October 2024. Gallup.com. https://news.gallup.com/poll/651977/americans-trust-media-remains-trend-low.aspx [Accessed: 25 March 2025].

Garcia, L. (2024) *Democracy Index: conflict and polarisation drive a new low for global democracy*. 15 February 2024. Economist Intelligence Unit. https://www.eiu.com/n/democracy-index-conflict-and-polarisation-drive-a-new-low-for-global-democracy/ [Accessed: 22 February 2024].

Gentile, G. & Pollicino, O. (2025) *How the US threw out any concerns about AI safety within days of Donald Trump coming to office*. 11 March 2025. The Conversation. http://theconversation.com/how-the-us-threw-out-any-concerns-about-ai-safety-within-days-of-donald-trump-coming-to-office-251659 [Accessed: 16 March 2025].

Ghosh, D. & Scott, B. (2018) *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet*. January 2018. New America. http://newamerica.org/pit/policy-papers/digitaldeceit/ [Accessed: 15 March 2025].

Gillespie, T. (2018) Google-Books-ID: cOJgDwAAQBAJ. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Haggart, B., Scholte, J. & Tusikov, N. (2024) *Power and Authority in Internet Governance: Return of the State?*

Hubbard, S. (2024) The Role of AI in the 2024 Elections. https://ash.harvard.edu/resources/the-role-of-ai-in-the-2024-elections/.

Jahn, L., Rendsvig, R.K. & Stærk-Østergaard, J. (2023) *Detecting Coordinated Inauthentic Behavior in Likes on Social Media: Proof of Concept*. doi:10.48550/arXiv.2305.07350.

Jeangène Vilmer, J.B., Escorcia, A., Guillaume, M. & Herrera, J. (2018) *Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff* (*CAPS*) *of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research* (*IRSEM*) *of the Ministry for the Armed Forces*. Paris. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

Johns Hopkins University, Imperial College London & Georgia Institute of Technology (2021) *NATO Review - Countering disinformation: improving the Alliance's digital resilience*. https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

Kang, C. (2017) F.C.C. Repeals Net Neutrality Rules. *The New York Times*. 14 December. https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html.

Kaska, K., Beckvard, H. & Minárik, T. (2019) *Huawei, 5G and China as a Security Threat*.

Klimburg, A. (2017) *The Darkening Web: The War for Cyberspace*. Penguin Press. https://hcss.nl/news/the-darkening-web-the-war-for-cyberspace/.

Kovalčíková, N. & Spatafora, G. (2024) *The future of democracy: lessons from the US fight against foreign electoral interference in 2024 | European Union Institute for Security Studies*. https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024.

Krekó, P. (2025) Brainwashing of the People, by the People, with the People. 28 February 2025. Authlib. https://www.authlib.eu/peter-kreko-mass-persuasion-systemic-disinformation/.

Krishnan, N., Gu, J., Tromble, R. & Abroms, L.C. (2021) Research note: Examining how various social media platforms have responded to COVID-19 misinformation. *Harvard Kennedy School Misinformation Review*. doi:10.37016/mr-2020-85.

Malingre, V. (2025) European digital regulation comes under attack from Trump, Musk and Zuckerberg. https://www.lemonde.fr/en/economy/article/2025/01/13/european-digital-regulation-comes-under-attack-from-trump-musk-and-zuckerberg_6737001_19.html.

Mansell, R., Durach, F., Kettemann, M., Lenoir, T., Procter, R., Tripathi, G. & Tucker, E. (2025) *Information Ecosystems and Troubled Democracy. A Global Synthesis of the State of Knowledge on News Media, AI and Data Governance*. Paris, International Observatory on Information and Democracy. https://observatory.informationdemocracy.org/report/information-ecosystem-and-troubled-democracy/.

Martinescu, A.-L., Stallard, S., Balatchi-Lupascu, A., Forlafu, M.G. & Osavul Data Team (2024) *Networks of Influence: Decoding foreign meddling in Romania's elections*. https://fpc.org.uk/networks-of-influence-decoding-foreign-meddling-in-romanias-elections-a-collaborative-investigation-into-disinformation-campaigns-and-influence-operation/.

Munteanu, D. (2024) Weathering the Disinformation Storm in 2024's Electoral Context, in: The 20th International Scientific Conference "Technologies, Military Applications, Simulation And Resources". In: *The 20th International Scientific Conference "Technologies, Military Applications, Simulation And Resources"*. April 2024 Bucharest, "Carol I" National Defence University Publishing House. pp. 80–88. doi:1053477-3045-1396-24-09.

Napoli, P.M. (2019) *Social Media and the Public Interest: Media Regulation in the Disinformation Age*. Columbia University Press.

NATO (2025) *Approche de l'OTAN pour la lutte contre les menaces informationnelles*. 5 February 2025. NATO. https://www.nato.int/cps/fr/natohq/topics_219728.htm [Accessed: 17 March 2025].

NATO (2021) *Brussels Summit Communiqué issued by NATO Heads of State and Governmen*t (*2021*). https://www.nato.int/cps/en/natohq/news_185000.htm.

NATO (2024a) *Hybrid Threats and Hybrid Warfare*. June 2024. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf [Accessed: 15 March 2025].

NATO (2024b) *NATO Allies agree common approach to counter information threats*. 18 October 2024. NATO. https://www.nato.int/cps/en/natohq/news_230522.htm [Accessed: 17 March 2025].

NATO (2023a) *NATO's approach to countering disinformation*. 2023. NATO. https://www.nato.int/cps/en/natohq/topics_219728.htm [Accessed: 23 February 2024].

NATO (2023b) *NATO's response to hybrid threats*. 23 April 2023. NATO. https://www.nato.int/cps/en/natohq/topics_156338.htm [Accessed: 28 May 2023].

NATO, E.C., European Council (2023c) *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 10 January 2023. NATO. https://www.nato.int/cps/en/natohq/official_texts_210549.htm [Accessed: 30 May 2023].

Pop, V., Dunai, M. & Ivanova, P. (2024) How Russia-backed influencers meddled in Romania's vote. *Financial Times*. 9 December. https://www.ft.com/content/4b00e7ec-2c79-4313-b012-4f09f436f3ed.

Quinn, B. & Milmo, D. (2024) How the far right is weaponising AI-generated content in Europe. *The Guardian*. 26 November. https://www.theguardian.com/technology/2024/nov/26/far-right-weaponising-ai-generated-content-europe.

Ray, T. (2025) *From Facebook to the little red book: Platform regulation under Trump 2.0*. https://www.orfonline.org/expert-speak/from-facebook-to-the-little-red-book-platform-regulation-under-trump-2-0.

Reflection Group Appointed by the Secretary General (2020) *NATO 2030: United for a New Er*a. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Reporters Without Borders (2020) *2020 World Press Freedom Index: "Entering a decisive decade for journalism, exacerbated by coronavirus" | RSF*. https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus.

Richardson, J. & Milovidov, E. (2019) *Digital citizenship education handbook: being online, well-being online, rights online*. Strasbourg, Council of Europe.

Richter, J.L., Brandon, D.I., Rowings, S.A., Hiner Antypas, V., Calascione, J.S. & Sriram, S. (2025) *President Trump's Freedom of Speech Order Takes Aim at Social Media, Broadcasters*. 27 January 2025. Akin Gump Strauss Hauer & Feld LLP - President Trump's Freedom of Speech Order Takes Aim at Social Media, Broadcasters. https://www.akingump.com/en/insights/alerts/President-Trumps-Freedom-of-Speech-Order-Takes-Aim-at-Social-Media-Broadcasters [Accessed: 15 March 2025].

Romanian Presidential Administration (2024) *Declassified information regarding interferences in the 2024 Romanian elections*. 4 December 2024. https://www.presidency.ro/ro/media/comunicate-de-presa/comunicat-de-presa1733327193 [Accessed: 12 February 2025].

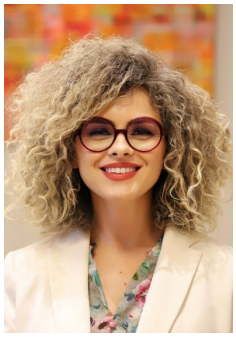
U.S. Government Accountability Office (2024) *Foreign Disinformation: Defining and Detecting Threats*. https://www.gao.gov/assets/880/871853.pdf.

Wardle, C. & Derakhshan, H. (2017) INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making. *Council of Europe Publishing*.

Windwehr, S. (2025) *Trump vs. Europe: The role of the Digital Services Act | Heinrich Böll Stiftung | Brussels office - European Union*. 18 February 2025. https://eu.boell.org/en/2025/02/18/trump-vs-europe-role-digital-services-act [Accessed: 16 March 2025].

Wonka, A., Gastinger, M. & Blauberger, M. (2025) The domestic politics of EU action against democratic backsliding: public debates in Hungarian and Polish newspapers. *Journal of European Public Policy*. 32 (2), 498–521. doi:10.1080/13501763.2023.2279245.

Zuboff, S. (2023) The Age of Surveillance Capitalism. In: *Social Theory Re-Wired*. 3rd edition. Routledge. p.



Daniela MUNTEANU is a researcher with the Euro-Atlantic Resilience Centre of the Romanian Ministry of Foreign Affairs and an associate lecturer at the National University of Political Studies and Public Administration. Her work focuses on strategy and policy drafting on societal resilience to information manipulation and hybrid threats. She also contributes to capacity-building projects focusing on resilience for the public sector. Daniela has acted as a researcher, coordinator and trainer on enhancing societal resilience in projects that brought together academia and government, resulting in public policy proposals on disinformation, hybrid threats and institutional resilience. As a capacity-building expert, she offers training on bolstering societal and institutional resilience to national and international government officials and civil servants. For the past years, she has also acted as trainer and facilitator for international courses organised under the auspices of the European Security and Defence College (ESDC) and NATO.